DEPARTMENT OF THE AIR FORCE AFMS 38BB
Headquarters, US Air Force
Washington DC 20330 11 October 1994

C4 SYSTEMS SECURITY ELEMENT

1. Mission Statement. The C4 Systems Security element provides all system security services required by the wing and other base activities. These services include: Computer Security (COMPUSEC), TEMPEST, Unit Information Security Manager, Communication-Computer (C-4) Security Education and Training Awareness Program (ETAP), Communication Security (COMSEC) Management, COMSEC Account Operations, and COMSEC Controlling Authority responsibilities.

2. Responsibilities:

2.1. Computer Security. Provides an acceptable level of protection for hardware, software, and classified, sensitive unclassified or critical data, material, or processes in the system. It compliments the other C4 security disciplines.

2.2. TEMPEST. Determines the required level of TEMPEST protection for electronic, electrical, or electromechanical systems, acquired facilities or equipment that processes classified information for all base users. Determines specific RED/BLACK installation requirements using the guidelines in TEMPEST regulations.

2.3. Unit Information Security Manager. Manages the units information, industrial, and personnel security programs. The duties include classification management, security clearances, eligibility determinations for access to classified information, safekeeping and storage, and contractor support of established classified contracts.

2.4. Communication-Computer (C4) Security Education and Training Awareness Program (ETAP). Provides base wide initial and refresher ETAP awareness training for all base personnel, distributes training and awareness materials and visual aids, provides specific guidance, and performs periodic staff assistance visits to unit ETAP monitors to ensure compliance with ETAP objectives.

2.5. Communications Security (COMSEC) Account Management. Manages all cryptographic material assigned to its locations. This includes receiving, distributing, inventorying, and destroying cryptographic material; training and assisting users; ensuring security practices are followed; inspecting users; and ensuring constant accountability of assets.

2.6. COMSEC Accounts Operations. Requisitions material for its users. Receives all COMSEC material, processes all vouchers, updates inventories, conducts daily, special and semiannual inventories, page checks all COMSEC material in the account, pulls material for transfer and prepares transfer correspondence.

2.7. Secure Telephone Unit (STU-III) Management. Manages the STU-III keying program. This includes receiving, distribution, inventorying, and destroying STU-III key; training and assisting COMSEC Responsible Officer(CRO)/STU-III Responsible Officer(SRO); and ensuring constant accountability of assets. Maintains files of National Security Agency(NSA) STU-III bulletins, Air Force Command Authority messages, regulations and other directives pertaining to STU-III operations and security. Register STU-III users, assign privileges, and order STU-III key.

3. Authority. National Security Agency directives, DOD directives, AFPD 33-2, C4 Systems Security, AFI 33 series, AFPD 31 series, contain policy and guidance for the C4 Security element.

____
No. of Pages: 14
OPR: AFMEA/PLDP
OCR: AFCOMMET/MOMC
Distribution: F

4. Applicability. This applies to objective wing C4 Systems Security Elements (Communications Squadrons only) in AMC, ACC, USAFE, PACAF, and ATC UPT bases during peacetime. It does not apply to the Air National Guard or the Air Force Reserve or to locations where a cost comparison study (OMB Circular A-76) was conducted.

5. Core Composition:

5.1. The assumptions considered to determine the core manpower required for C4 Security were an objective wing of 72 Primary (F16s) Aircraft Assigned, a base population of 3055, 850 personal computers (+/- 10%), 15 personal computers used for classified processing, 23 COMSEC Users, 772 Line Items, supporting the following offices:

5.1.1. Wing

5.1.2. Operations Group

5.1.3. Operations Support Squadron

5.1.4. Operations Squadron

5.1.5. Maintenance Squadron

5.1.6. Security Police Squadron

5.1.7. Communications Squadron

5.2. Core Composition Variable. Increased authorizations in base population are assumed to support an increase of aircraft assigned. An increase in base population, without additional aircraft, will increase the manpower required for COMPUSEC, TEMPEST, Comm-Computer Security Education Training & Awareness Program (ETAP). These increases are also assumed to increase at a rate of 24 aircraft and 400 personnel at a time. To support a single incremental increase of this size, one additional manpower authorization is required.

5.3. Core Manpower Required. 4

5.4. Core Range. 3 - 11

5.5. Programming Factor. Base Population.

6. Standard Data:

6.1. Classification. Type III

6.2. Approval Date. 1 March 1993

6.3. Man-Hour Data Source. Workshop

6.4. Man-hour Equation: $Yc = 252.58 + .1015(X)$

6.5. Workload Factor:

6.5.1. Title. Authorized Population.

6.5.2. Definition. The average monthly number of personnel authorized to the installation. Include all funded civilian (US and Foreign) and military authorizations in all host and tenant units serviced by the local communications unit. Do not include CMEs in determining the requirement. However, if the work center is providing direct support to a contractor work force, a variance should be developed to account for this workload. Do not include a population count for those agencies which are covered under the specific approved variances listed at attachment 3.

6.5.3. Source. The Unit Manpower Documents (UMDs) for the installation or other Air Force programming documents.

6.6. Study Team:

6.6.1. Study Leader. Mr. Larry Carmack, AFCOMMET/MOMM.

6.6.2. Functional Representative. Mr. J.J. Plummer, TIC/DS

6.6.3. Program Manager. Msgt Dennis Deas, HQ AFMEA/MEMS

7. Application Instructions:

7.1. Determine the authorized population by summing the last fiscal quarter authorized tables for all units supported by the installation. Substitute figure for "X" in the man-hour equation.

7.2. Determine the variance man-hours applicable to your location.

7.3. Add/subtract the man-hours obtained from 7b to man-hours obtained from 7a.

7.4. Divide the resulting man-hours by the Man-hour Availability Factor (MAF) and overload factor and use current rounding rules to determine whole manpower requirements.

7.5. Refer to the Manpower Table at Attachment 2 to determine the skill and grade requirement.

8. Statement of Condition. This element has no conditions that impact it's ability to perform work identified in the Element Description.

PUBLISHED UNDER THE AUTHORITY OF THE SECRETARY OF THE AIR FORCE

4 Atch
1. Element Description
2. Standard Manpower Table
3. Variances
4. Process Analysis Summary

ELEMENT DESCRIPTION

C4 SECURITY

1. COMPUTER SECURITY:
1.1. PROVIDES ADVICE AND GUIDANCE. Provides advice and guidance to the Computer Facility Manager (CFM), Communications-Computer Security Officer (CSSO), and unit personnel.
1.2. ACTS AS ACCREDITATION ADVISOR. Acts as accreditation advisor to the designated approving authority (DAA).
1.3. PROVIDES INPUT TO SECURITY PROGRAM. Provides input to the host base security programs.
1.4. ACTS AS CHAIRPERSON. Acts as the base Computer Security Working Group chairperson.
1.5. DEFINES AND ASSESSES SECURITY REQUIREMENT. Defines and assesses every security requirement for new or upgraded systems to support the base mission(s).
1.6. PROVIDES THREAT ASSESSMENT. Provides threat assessment of proposed and established systems when the threat changes.
1.7. DEVELOPS, IMPLEMENTS, AND CHANGES THE RISK MANAGEMENT PROCESS. Develops, implements, and changes the risk management process used to support requests for approval from the DAAs.
1.8. PARTICIPATES AS A MEMBER OF THE COMMUNICATIONS-COMPUTER SYSTEMS REQUIREMENT BOARD (CSRB). Reviews CSRD to insure security is addressed in all requests for a new system or modification to an existing system. Attends CSRB.
1.9. ATTENDS CONFERENCE AND WORKSHOP. Attends computer security conference and workshop to maintain currency on the latest security techniques.
1.10. DEVELOPS AND PUBLISHES COMPUTER SECURITY PROCEDURE. Develops and publishes base-wide computer security procedures (newsletters, OIs, etc.).
1.11. OBTAINS APPROVAL FOR BASE UNITS TO PROCESS CLASSIFIED AND/OR SENSITIVE UNCLASSIFIED INFORMATION OR OPERATE CRITICAL SYSTEM. Obtains written approval from DAA to allow base units to process classified and/or sensitive unclassified information or operate a system.
1.12. ENSURES APPOINTMENT OF CFM. Verifies all computer facilities have a CFM assigned.
1.13. ENSURES TERMINAL AREA SECURITY OFFICER (TASO) IS APPOINTED. Ensures TASO is appointed for each personal computer and terminal with dial-up capability, and each remote terminal.
1.14. REVIEWS AND APPROVES COMPUTER SECURITY PROCEDURE. Reviews and approves every base computer security procedure for computer facilities, remote terminals, and work station areas.
1.15. ENSURES RISK ANALYSIS IS CONDUCTED. Ensures an adequate risk analysis is conducted for each computer facility and computer.
1.16. ENSURES COMPUTER FACILITY IS CERTIFIED. Reviews a CFM certification to insure a computer facility meets appropriate security specifications and ensures trusted facility manual and/or operational site security manual is developed and implemented.
1.17. ENSURES COMPUTER SECURITY MEASURES ARE RECERTIFIED. Ensures all computer facility security measures are recertified at least every three years, or upon significant systems modification, and ensures trusted facility manual and/or operational site monitors security manual is developed and implemented.
1.18. MONITORS PERSONNEL SECURITY TRAINING. Ensures all base personnel who operate computers receive security training.
1.19. FOLLOWS UP ON SECURITY INCIDENT. Ensures each security incident is reported and appropriate action is taken.
1.20. MONITORS COMPUTER FACILITY ACTIVITY. Monitors computer facility activity to ensure compliance with security procedures.
1.21. PREPARES AND SUBMITS ANNUAL COMPUTER SECURITY POSTURE
REVIEW TO HIGHER HEADQUARTERS.
1.22. REVIEWS SYSTEM AND NETWORK. Reviews every computer system and network configuration change, system component change, or modification to ensure system security is not degraded.
1.23. PREPARES, BRIEFS, AND/OR ADVISES SECURITY POSTURE. Prepares briefing and/or advises the CFM and unit commander on security posture.
1.24. VERIFIES LIST OF NETWORK SECURITY MANAGERS (NSMs)/OFFICERS (NSOs).

1.25. SCHEDULES, PREPARES FOR, AND CONDUCTS STAFF ASSISTANCE VISIT.
1.26. PROVIDES FUNCTIONAL AREA COMPUTER USER SECURITY TRAINING. Provides training to each NSM, CCSO, SFM, TASO and other persons who use computers.

2. TEMPEST:
2.1. ATTENDS PLANNING MEETING. Attends each base planning meeting.
2.2. PERFORMS TEMPEST COUNTERMEASURES ASSESSMENT. Performs countermeasures assessment in accordance with AFPD 33-2, National Telecommunications and Information System Security Instruction (NTISSI) 7000.
2.3. CONSTRUCTION OR REHABILITATION PROJECT. Conducts on-site visual inspection and prepares report.
2.4. PROVIDES INSTALLATION STAFF TEMPEST TECHNICAL ASSISTANCE WHEN REQUIRED/REQUESTED. Reviews TEMPEST criterion and processes request for TEMPEST test. Reviews result of TEMPEST test and processes risk acceptance request.
2.5. RESEARCHES, REVIEWS, DEVELOPS, AND SUBMITS DIRECTIVE FOR PUBLICATION. Researches, reviews, develops, submits, and maintains a TEMPEST directive that provides guidance and assigns duties and responsibilities.
2.6. DISSEMINATES TEMPEST INFORMATION. Disseminates higher headquarters and base TEMPEST policy, guidance, and general information to both the base unit representatives and the general base population.
2.7. CONDUCTS INITIAL RED/BLACK TEMPEST INSPECTION. Prepares, conducts, documents, reports, and briefs inspection results whenever equipment is added to or reconfigured within a facility that processes NSI.
2.8. CONDUCTS ANNUAL RED/BLACK TEMPEST INSPECTION. Prepares, notifies, conducts, documents, reports, and briefs inspection results for all facilities and equipment which process NSI.
2.9. CONDUCTS FOLLOW-UP RED/BLACK TEMPEST INSPECTION. Prepares, notifies, conducts, documents, reports, and briefs inspection results and/or status of corrective action.
2.10. ASSISTS BASE CONTRACTING OFFICER. Assists the base contracting officer in developing applicable standard necessary for contractual compliance with TEMPEST requirement.
2.11. REVIEWS PROJECT PACKAGE. Reviews each site concurrence letter (SCL), SCL change, and scheme package for facilities that will process NSI, and recommends change, addition, and approval/ disapproval.
2.12. COORDINATES ON SCHEME ACTION. Coordinates on AF Form 1261, Information System Acceptance, Commissioning, and Removal Certificate, for any scheme action when NSI is to be processed.
2.13. DEVELOPS AND MANAGES EDUCATION PROGRAM. Develops and manages the base TEMPEST security education program.
2.14. CONDUCTS STAFF ASSISTANCE VISIT. Conducts TEMPEST staff assistance visit to base, subordinate detachment, and operating location.

3. UNIT INFORMATION SECURITY MANAGER:
3.1. PROVIDES UNIT CLASSIFICATION MANAGEMENT. MONITORS ORIGINAL CLASSIFICATION AUTHORITY (OCA) REQUIREMENT. PROCESSES OCA DELEGATION REQUEST. Ensures OCA is not delegated to a person who only reproduces, extracts, or summarizes classified information, or who only applies classification markings derived from source material or as directed by security classification guide, and provides recommendation to unit commander and sends evaluation to higher headquarters. CONDUCTS UNIT ANNUAL OCA LIST REVIEW. Examines list, determines if OCA has demonstrated continuing need for authority, and sends report to host higher headquarters when OCA is no longer required.
3.2. PROCESSES C-4 SYSTEMS SECURITY CLASSIFICATION GUIDANCE.
COORDINATES ON UNIT SECURITY CLASSIFICATION GUIDANCE. Reviews security classification guide, plan, operations order, program, or project document to ensure guidance identifies information elements requiring protection, classification designation to be applied to each element, and declassification instructions which pertain to each information element. PROCESSES UNIT BIENNIAL REVIEW OF SECURITY CLASSIFICATION GUIDE. Ensures guide is reviewed for currency and accuracy at least once every two years, and sends results to higher headquarters.
3.3. SAFEGUARDS UNIT CLASSIFIED INFORMATION. PERFORMS UNIT PROGRAM REVIEW. Conducts annual program review of each function, including subordinate detachments and operating locations serviced, to determine status of classification management, safeguarding classified information, security education, industrial

security, and personnel security programs. Reviews TOP SECRET procedure. Reviews SIOP procedure. Reviews SCI procedure. Reviews NATO procedure. Reviews OTHER procedure.

3.4. CONDUCTS UNIT PHYSICAL SECURITY SURVEY. Conducts survey of each function, including subordinate detachments and operating locations serviced to determine requirements for, or compliance with, security policies and procedures for protecting classified information. Evaluates Unit Secure conference room. Evaluates Unit Top Secret storage facility. Evaluates Unit SIOP-ESI storage facility. Evaluates Unit NATO storage facility. Evaluates Unit OTHER storage facility.

3.5. MONITORS SECURITY INCIDENT AND/OR BREACHES OF SECURITY AS DIRECTED BY DoD 5200.1-R/AFPD 34-1, INFORMATION SECURITY PROGRAM. Monitors preliminary inquiry or formal investigation, provides written review of security incident report, and sends report through command channels.

3.6. PREPARES UNIT PROGRAM DATA REPORT. Disseminates higher headquarters instructions, consolidates input, and prepares and submits final report.

3.7. PROCESSES UNIT WAIVER REQUEST. Ensures waiver request for storage requirement is complete and evaluates it, forwards the evaluation and request to higher headquarters, performs annual evaluation/follow-up of the request, and takes action.

3.8. PROCESSES UNIT REQUEST FOR ACCESS. Ensures access by a person outside the Executive Branch of the US Government (e.g., congressional inquiries, freedom of information act, etc.) is required, and determines release of information is not prohibited by originating agency.

3.9. MAINTAINS SCI DOCUMENTATION; MAINTAINS UNIT SCI BILLET (SCIB) ROSTER. Ensures SCI nominations, indoctrinations, codings of UMDS, reports, debriefings, terminations or suspensions, and for cause discharge actions are reported through Command Channels.

3.10. MONITORS SPECIAL ACCESS PROGRAM (SAP). Ensures unit access procedures for Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI), Critical Nuclear Weapon Design Information (CNWDI), or other SAPs the unit may be involved with or have access to, conform to the policies and procedures prescribed by the respective directive.

3.11. CONTROLS UNIT FOREIGN DISCLOSURE. Ensures Air Force information (classified and unclassified) is not released to foreign nations until prescribed command releases authority is obtained.

3.12. MONITORS UNIT INDUSTRIAL SECURITY. ASSISTS IN PREPARATION OF CONTRACTOR VISITOR GROUP SECURITY SUPPORT AGREEMENT. Assists in the preparation of security support agreement between US Government and contractor management personnel. Reviews Unit Contract Documentation. Coordinates on security requirements relating to classified contractor performance. Coordinates on Unit DD Form 254, Contract Security Classification Specification. Ensures guidance is accurate for classified contract performance, and performs biennial review of each contract security classification specification. PROCESSES/MONITORS UNIT VISITOR REQUEST. Processes and monitors all requests by contractor personnel to visit unit facilities, and prepares and submits annual report of Contractor Visitor Groups to higher headquarters. PERFORMS UNIT CONTRACTOR VISITOR GROUP INDUSTRIAL SECURITY INSPECTION. Performs inspection of each classified contract to determine effectiveness of contractor's security program. Performs Initial Inspection. Performs Recurring Inspection. Performs Unannounced Inspection. Performs Follow-up Inspection. Performs Closeout Inspection. PROVIDES UNIT BRIEFING. Provides access briefing to selected contractor personnel, and provides defensive (foreign travel) security briefing for all cleared contractor personnel.

3.13. MONITORS UNIT PERSONNEL SECURITY. PERFORMS QUALITY CHECK OF UNIT INVESTIGATION REQUEST PACKAGE. Determines if investigation is warranted and ensures all member and unit generated forms contain required information.

3.14. PROCESSES ACCESS DOCUMENTATION. PROCESSES CONTROLLED AREA AND RESTRICTED AREA BADGE DOCUMENTATION. Reviews documentation, determines accuracy, and coordinates. Issues Unit Access Badge. Issues local unit access badge. Processes Access Documentation. Review documentation, determines accuracy, and coordinates. PROVIDES SECURITY TERMINATION STATEMENT/DEBRIEFING. Issues Security Termination Statement form, conducts debriefing, and obtains signature. PERFORMS ANNUAL INVENTORY OF CONTROLLED AREA AND RESTRICTED AREA BADGES. Writes cover letter, forwards inventory listing to work centers, reviews annotated listing and forwards corrected copy to Base Security Police (SP).

3.15. CONDUCTS FOREIGN TRAVEL BRIEFING. Briefs personnel departing on overseas travel about travel risk/terrorist activities in travel area.

3.16. RESPONDS TO INQUIRY. Answers unit question on clearance matters, including submission of tracer action.

3.17. REVIEWS UNIT MONTHLY AUTOMATED SECURITY CLEARANCE APPROVAL SYSTEM (ASCAS) PRODUCT AND RESOLVES DISCREPANCY WITH HOST BASE SECURITY POLICE. MONITORS UNIT INVESTIGATION PROCESS. Monitors investigation progress until completed or canceled. Forwards Unit Suspense Copy on PCS Personnel to gaining installation. Forwards all information relating to pending clearances to gaining installation.
3.18. PROCESS UNIT LIMITED ACCESS AUTHORIZATION FOR IMMIGRANT ALIENS. Ensures request for limited access is complete and forwards to approving authority. Monitors authorization to ensure it does not exceed imposed expiration date.
3.19. ADMINISTERS UNIT PRESIDENTIAL SUPPORT PROGRAM. Submits nomination file to Air Force Security Clearance Office (AFSCO), maintains file of assigned positions, and sends report to higher headquarters when member is no longer qualified for Presidential Support duties.
3.20. PREPARES UNIT REPORT. Prepares adverse action report when member is denied special access or assignment to personnel reliability program position based on Defense Investigative Service (DIS) report of investigation, and notification of higher headquarters when member refuses to execute security termination statement.
3.21. PREPARES UNIT SUBVERSIVE ACTIVITIES REPORT AND FORWARDS TO HOST BASE OFFICE OF SPECIAL INVESTIGATIONS (OSI).
3.22. PROVIDES UNIT INFORMATION TRAINING; PROVIDES INITIAL TRAINING. Provides initial unit training for information, personnel, and industrial security. PROVIDES ANNUAL/RECURRING TRAINING. Provides annual/recurring unit training for information, personnel, and industrial security.
3.23. PROVIDES UNIT TECHNICAL GUIDANCE. Provides requested technical guidance to the unit on any and all information security matters.

4. C-4 SECURITY EDUCATION AND TRAINING PROGRAM (ETAP):
4.1. MANAGES ETAP. Prepares education and training materials, and provides program publicity relating to the ETAP.
4.2. CONDUCTS AND DOCUMENTS INITIAL/RECURRING ETAP TRAINING OF ALL UNIT ETAP MONITORS.
4.3. CONDUCTS UNIT ETAP MONITOR MEETING. Conducts ETAP monitor meeting.
4.4. CONDUCTS UNIT INITIAL ETAP MONITOR TRAINING. Conducts
initial training for unit personnel appointed security monitor.
4.5. EVALUATES UNIT ETAP PROGRAM. Performs annual staff assistance visit to ensure ETAP objectives are being met.
4.6. DISSEMINATES ETAP MATERIAL. Disseminates ETAP material received from higher headquarters to unit ETAP monitors.
4.7. MAINTAINS ETAP CONTINUITY FOLDER. Maintains a ETAP continuity folder that includes implementing directives, appointment letters, points of contact, sample reports and letters, a listing of policies and responsibilities, and hands-on procedures.

5. COMSEC ACCOUNT MANAGEMENT:
5.1. COMPLIES WITH INSPECTION REQUIREMENT/PERFORMS INSPECTIONS.
CONDUCTS USER ACCOUNT INSPECTION. Prepares for user inspection, conducts briefing, performs inspection and documents each finding, prepares inspection report and forwards to user, and reviews user response and follows up. CONDUCTS ACCOUNT SELF INSPECTION. Prepares for account self inspection, conducts briefing, performs inspection, documents each finding, provides references, merges findings from user inspections, prepares inspection report and initiates corrective actions.
5.2. SUPPORTS COMMAND INSPECTION. Notifies affected agency, gathers material, arranges transportation and billeting for inspection team, accompanies command inspector at user location
and COMSEC account, and attends briefing. TAKES FOLLOW-UP ACTION. Establishes suspense for corrective action, reviews corrective action taken for concurrence/nonconcurrence, submits subsequent follow-up report, prepares and submits close-out letter, and files inspection report.
5.3. MAINTAINS RECORD. Reviews record, folder, or file content for compliance with directives and takes disposition action, as required. Maintains seven-part folder. Maintains inventory record. Maintains policy/procedure folder. Maintains access control record. Maintains insecurity folder. Maintains waiver folder.

5.4. MAINTAINS CERTIFICATION FILE. Maintains Maintenance Modification certification file. Maintains Secure Voice certification file. Maintains Plan certification file. Maintains Vault certification file. Maintains Personnel certification file.
5.5. MAINTAINS ACCOUNT IDENTIFICATION FILE.
5.6. MAINTAINS SURVEY FILE.
5.7. MAINTAINS CONTINUITY FOLDER.
5.8. CONDUCTS RESEARCH FOR AVAILABLE ASSET. Receives inquiry, researches material availability, analyzes information gathered, drafts and submits response to inquiry.
5.9. PROCESSES SURVEY REPORT. REVIEWS CORRESPONDENCE ON SURVEY REPORT. Reviews recurring/non-recurring survey requirement, schedules survey with affected agency, and prepares and submits survey request to affected agency. CONDUCTS SURVEY. Prepares and conducts briefing, conducts survey, and compiles survey data. PREPARES SURVEY RESPONSE. Establishes and monitors survey suspense data, reviews compiled survey data, prepares and submits survey report, and takes follow-up action, as required.
5.10. PERFORMS COMSEC INCIDENT REPORTING PROCEDURES. PREPARES INITIAL REPORT. Conducts or reviews preliminary inquiry, prepares and submits initial incident report upon notification of an incident. SUBMITS INCIDENT INVESTIGATIVE OFFICER APPOINTMENT LETTER. Coordinates appointment with responsible office, verifies appointee security status, prepares and submits letter of appointment to commander. MONITORS INCIDENT REPORTING. Maintains incident log, establishes suspense date, reviews correspondence on incident, and monitors incident investigation. SUBMITS INTERIM/ FOLLOW-ON INCIDENT REPORT. Compiles additional facts on incident, prepares and submits interim/follow-on incident report to action agency. SUBMITS INCIDENT FINAL REPORT. Reviews incident inquiry/investigative report; reviews commander's comment on incident; prepares custodian comment; drafts, coordinates, and submits incident final report to action agency.
5.11. SUBMITS YEARLY LETTER TO MAJCOM COMMANDER. Extracts and complies data from incident reports; prepares and submits letter to MAJCOM Commander on commonality of causes of incidents and actions taken to prevent future incidents.
5.12. DEVELOPS AND MAINTAINS EMERGENCY ACTION PLAN (EAP). Researches requirement, drafts and coordinates draft and EAP with effected agencies, tests draft, prepares final copy, publishes and distributes EAP to action agencies. Reviews EAP for currency, and performs dry runs.
5-13. REVIEWS COMSEC ACCOUNT REQUIREMENTS. Reviews program document, COMSEC account holdings, and Operations Plan/Operations Order (OPLAN/OPORD) for currency; determines adequacy of requirements; prepares and submits recommendation for change to action agency.
5.14. PROCESSES WAIVER REQUEST. Reviews, researches, and validates waiver request; prepares and submits waiver or recommendation to action agency; and monitors waiver status.
5.15. PROCESSES SYSTEM REQUIREMENT REQUEST. Assists user in developing system requirement, researches system alternative, using various COMSEC regulations/publications and prepares and submits system requirement request to action agency.
5.16. PREPARES CHANGE OF CUSTODIAN. Requests special listing of holdings, performs change of custodian inventory, reviews all applicable letters and forms, coordinates EAP, performs account self inspection, changes each safe/vault combination, and prepares and submits listing of holdings to action agency.
5.17. DEVELOPS USER GUIDE. Researches applicable regulations and drafts, edits, and publishes user guide.
5.18. PUBLISHES SUPPLEMENT TO REGULATIONS. Conducts research, prepares and coordinates draft, prepares and staffs final copy, and publishes and distributes supplement to regulation.
5.19. PERFORMS REQUIRED CERTIFICATION/RECERTIFICATION OF EVERY USER. Reviews required directive, regulation, and publication, and documents certification/recertification action completed.
5.20. PERFORMS CONTROLLED AREA INSPECTION. Preforms inspection IAW directive/regulation, documents finding(s), prepares inspection report, and takes follow-up action.
5.21. PERFORMS SAFE/VAULT COMBINATION CHANGE. Maintains listing of every safe/vault combination and changes combinations as required.
5.22. MONITORS ACCESS ROSTER AND/OR AUTHORIZATION LIST. Reviews, updates, prepares, and certifies access roster/authorization list for the unit and each user account.

6. COMSEC ACCOUNT OPERATIONS:
6.1. CONTROLS COMSEC MATERIAL AND EQUIPMENT HANDLED THROUGH THE COMSEC MATERIAL CONTROL SYSTEM (CMCS).

6.2. REQUISITIONS MATERIAL OR EQUIPMENT. Validates request from user; prepares Irregularly Superseded COMSEC material (ISCOM), COMSEC, and equipment request; and submits requisition.
6.3. RECEIVES COMSEC MATERIAL OR EQUIPMENT; MEETS DELIVERY AGENT. Arranges transportation, loads/unloads material or equipment, checks package, and validates receipt.
6.4. RECEIVES TWO-PERSON CONTROLLED COMSEC MATERIAL; MEETS DELIVERY AGENT. Prepares authorization letter/message for two-person pick-up, arranges transportation, loads/unloads material, checks package, and validates receipt.
6.5. UNPACKS MATERIAL OR EQUIPMENT. Unpacks material or equipment and verifies completeness of content.
6.6. CHECKS DOCUMENT; PERFORMS UNSEALED DOCUMENT CHECK. Checks each page of unsealed document, identifies and marks sensitive page/document for destruction, and stamps and signs document. PERFORMS SEALED DOCUMENT CHECK. Checks sealed document, identifies and marks sensitive page/document for destruction, and stamps and signs document.
6.7. PROCESSES RECEIPT VOUCHER. Stamps and signs completed receipt voucher; updates AFCOMSEC Form 14, COMSEC Material-Voucher and Package Register; notifies COMSEC custodian; submits receipt voucher to action agency; and files receipt voucher. PUTS MATERIAL ON INVENTORY. Updates AFCOMSEC Form 16, COMSEC Account Daily-Shift Inventory, and/or AFCOMSEC Form 23, COMSEC Account Local Inventory Report.
6.8. REPORTS DISCREPANCY IN SHIPMENT. Prepares and submits report of discrepancy to action agency. Reports Two-Person Control Report of Discrepancy. Reports "No Listing of Document" discrepancy. Reports "Missing Page of Document" discrepancy.
Reports "Non-Receipt of Document" discrepancy. Reports "Duplicate or Misplaced Page in Document" discrepancy.
6.9. DISPOSES OF OR STORES PACKAGING MATERIAL. Removes classified marking, checks residue for classified material, disposes of residue, and stores reusable container.
6.10. STORES MATERIAL/EQUIPMENT. Prepares material/equipment for storage, seals package or container, places material/ equipment in approved storage location, and updates AFCOMSEC Form 16.
6.11. TRANSFERS MATERIAL OR EQUIPMENT; PREPARES AND SUBMITS TRANSFER CORRESPONDENCE. Reviews COMSEC requirement, reviews .padirected transfer requirement, prepares and submits transfer request, and notifies affected agency of two-person control shipment. PULLS MATERIAL OR EQUIPMENT FOR TRANSFER. Pulls material/equipment on hand, pulls material/equipment from user account, verifies completeness of material/equipment to be transferred, and removes material/equipment from inventory. PREPARES TRANSFER VOUCHER. Prepares unclassified/classified voucher, and updates AFCOMSEC Form 14. PREPARES MATERIAL/ EQUIPMENT FOR TRANSFER. Packages material/equipment, prepares packaging label, and prepares shipping document. PROCESSES MATERIAL/EQUIPMENT THROUGH SHIPPING AGENCY. Arranges for transportation, loads/unloads material/equipment, verifies identification of shipping agent, transfers control of package to shipping agent, and obtains signed receipt.
6.12. INVENTORIES COMSEC MATERIAL/EQUIPMENT. CONDUCTS DAILY INVENTORY. Gathers material, conducts daily inventory of single-person and two-person control items, and updates AFCOMSEC Form 16. CONDUCTS SEMIANNUAL INVENTORY. Gathers material, coordinates inventory schedule with all users, compares inventory listing against holding, and performs inventory. CONDUCTS SPECIAL/ EMERGENCY INVENTORY. Prepares inventory list of all holdings, gathers material, coordinates inventory schedule with all users, compares inventory listing against holding listing, and performs inventory.
6.13. PREPARES INVENTORY CORRESPONDENCE. Prepares supplemental inventory listing, updates custodian list, reconciles inventory listing, prepares and submits semiannual inventory report to controlling agency, and takes follow-up action, as required.
6.14. ISSUES MATERIAL/EQUIPMENT; REVIEWS USER REQUIREMENT. Pulls user folder, compiles worksheet, and checks status document. PREPARES MATERIAL/EQUIPMENT FOR ISSUE. Pulls material/equipment from storage location; updates inventory record; unwraps material as required; page checks unsealed document; and annotates document with status. PREPARES ISSUE DOCUMENT. Extracts information from source document to prepare SF Form 153, COMSEC Material Report used for issue document, for each user account and verifies issue document against source document for accuracy. PACKAGES MATERIAL/EQUIPMENT FOR ISSUE. Organizes material/equipment based on user requirement; packages material/equipment, as required; and updates inventory record. ISSUES MATERIAL/EQUIPMENT OVER THE COUNTER. Notifies user for pickup, verifies identity and authorization of recipient, issues material over-the-counter, obtains copy of signed hand receipt, and updates

inventory. FILES HAND RECEIPT. Reviews SF Form 153 used as hand receipt for completeness, inserts in user folder, and files user folder.
6.15. ROTATES MATERIAL IN SAFE. Moves material/equipment at 30-60-90 day rotation intervals to rotation location, updates inventory record, and color codes material for destruction priority.
6.16. PREPARES FOR DESTRUCTION; PERFORMS DESTRUCTION. Reviews source document, verifies status, schedules for destruction with facility monitor, coordinates schedule with user, and arranges transportation. PULLS MATERIAL TO BE DESTROYED. Pulls material from storage location, receives material from user, page checks material, verifies status, and updates inventory record.
PREPARES MATERIAL FOR DESTRUCTION. Prepares destruction report, removes staples, removes material from binders, crumples, and containerizes material to be destroyed. DESTROYS MATERIAL. Loads/unloads material; prepares destruction device, as required; places material in destruction device; ensures all material is destroyed; searches and cleans destruction facility, as required.
6.17. TAKES POST-DESTRUCTION ACTION. Signs destruction report; prepares and submits AFCSC Form 25, ISCOM Usage and Resupply Card, to issuing agency; adjusts inventory record; and files destruction report.
6.18. PROCESSES MONTHLY DESTRUCTION REPORT. Processes monthly destruction report; compares local destruction report against monthly report and annotates correction, deletion, or addition; and prepares supplemental voucher, as required.
6.19. PERFORMS REQUIRED TWO-PERSON CERTIFICATION/ RECERTIFICATION. Reviews required directive, regulation, and publication; and certifies/recertifies action completed. Performs Initial Certification. Performs Monthly Recertifica- tion. Performs Quarterly Recertification. Performs "When Directed" Recertification. Performs Two-Person Lock Certification/Recertification. Performs Two-Person Control Procedural Certification/Recertification.
6.20. MAINTAINS COMSEC DOCUMENT. Posts message/printed amendment; verifies posting for accuracy; page checks residue and document; prepares SF Form 153, used as Destruction Report; destroys residue; and requests replacement material.
6.21. PERFORMS FACILITY PROTECTION; PERFORMS TEST. Coordinates test with action agency, performs test, and maintains log of test. PERFORMS SAFE/VAULT COMBINATION CHANGE. Maintains listing of safe/vault combinations, and changes combination, as required.
6.22. PROCESSES MATERIAL/EQUIPMENT FOUND ON BASE (FOB). Retrieves material/equipment, determines accountability, stores material/equipment, adjusts inventory, and acts on disposition instruction.
6.23. PROCEDURAL INSTRUCTION AND CUSTOMER EDUCATION. PUBLISHES AND DISTRIBUTES USER GUIDE. Reproduces finalized copy of user guide, coordinates with user for pick-up of user guide, distributes user guide, and obtains "signature of receipt" from user. PROVIDES SYSTEM OPERATING INSTRUCTION. Schedules appointment with system user, prepares instructional material, and provides system operating instruction to user. PUBLISHES INFORMATION LETTER. Researches information; drafts, publishes, and distributes information letter to user.
6.24. PROVIDES CUSTOMER EDUCATION. PREPARES FOR CUSTOMER EDUCATION/ORIENTATION. Researches material; prepares education/ orientation outline; and schedules new user, two-person control, or two-person integrity user for education/orientation. CONDUCTS CUSTOMER EDUCATION/ORIENTATION. Sets-up classroom/presentation location, conducts customer education/orientation for new user, and documents attendance.
6.25. PERFORMS ASSISTANCE VISIT TO USER LOCATION. Reviews request, schedules visit, reviews user folder, arranges transportation, performs visit, documents visit and finding, and takes follow-up action, as required.
6.26. VICINITY TRAVEL. Performs vicinity travel to user, delivery agent, and destruction facility location to accomplish inspection, receipt of material/equipment, inventory, transfer of material/equipment, destruction of material, and assistance visit.

7. STU-III:
7.1. ADDS, MODIFIES, DELETES DEPARTMENT, AGENCY, ORGANIZATION (DAO) CODE. Accomplishes and submits STU-III DAO Registration Form. ADDS, MODIFIES, DELETES USER REPRESENTATIVES, ADDRESSES, TELEPHONE NUMBERS. Accomplishes and submits STU-III User Representative Registration Form. REQUESTS STU-III USER PRIVILEGES. Accomplishes and submits User Representative STU-III Privilege Registration Form.
7.2. PREFORMS STU-III COMSEC INCIDENT REPORTING PROCEDURE. PREPARES INITIAL STU-III COMSEC INCIDENT REPORT. Conducts preliminary inquiry; and prepares and submits initial incident report upon notification of incident. CONDUCTS INITIAL/FOLLOW-UP STU-III COMSEC INCIDENT BRIEFING. Prepares briefing, and briefs responsible office/individual. SUBMITS STU-III COMSEC INCIDENT INVESTIGATIVE OFFICER

APPOINTMENT LETTER. Coordinates appoint- ment with responsible office, verifies appointee security status; and prepares and submits letter of appointment to commander. MONITORS STU-III COMSEC INCIDENT REPORTING. Maintains incident log, establishes suspense date, reviews correspondence on incident, and monitors incident investigation. SUBMITS AMPLIFIED/FOLLOW-ON STU-III COMSEC INCIDENT REPORT. Complies additional facts on incident; and prepares and submits amplified/ follow-on incident report to required agencies. SUBMITS STU-III COMSEC INCIDENT FINAL REPORT. Reviews incident inquiry/ investigative report; reviews commander's comments on incident; prepares custodian comment; and drafts, coordinates, and submits incident final report to required agencies.

7.3. MAINTAINS FILES. Maintains a file of NSA STU-III Bulletins; Air Force Command Authority Messages, NSA Keynotes, policy messages, regulations and other directives pertaining to STU-III operations and security.

7.4. RECEIVES STU-III FILL DEVICE. REQUISITIONS FILL DEVICE. Validates request from user and submits requisition. RECEIVES FILL DEVICE FROM DELIVERY AGENT. Loads/unloads material, checks package, and validates receipt. RECEIVES FILL DEVICE BY REGISTERED MAIL. Receives package and validates receipt. UNPACKS FILL DEVICE. Unpacks fill device and verifies completeness of content. PROCESSES RECEIPT VOUCHER. Stamps and signs completed receipt voucher; updates AFCOMSEC Form 14; submits receipt voucher to required agencies and files receipt voucher. STORES FILL DEVICE. Places fill device in approved storage location and updates inventory record.

7.5. PROVIDES STU-III USER EDUCATION/ORIENTATION. PREPARES FOR STU-III USER EDUCATION/ORIENTATION. Researches material; prepares education/orientation outline; and schedules user for education/orientation. CONDUCTS STU-III USER EDUCATION/ ORIENTATION. Sets-up classroom/presentation location, conducts education/orientation for user and documents attendance.

7.6. PERFORMS STAFF ASSISTANCE (SAV) TO STU-III USER LOCATION; PREPARES FOR SAV. Reviews request, schedules visit, and reviews user folder. PERFORMS AND DOCUMENTS SAV. Performs visit, documents visit and finding, and takes follow-up action as required.

7.7 PERFORMS VICINITY TRAVEL. Performs vicinity travel to support STU-III users.

STANDARD MANPOWER TABLE

WORK CENTER/FAC	APPLICABILITY MAN-HOUR RANGE
C4 SECURITY/38BB	387.83 - 2089.10

AIR FORCE SPECIALTY TITLE	AFSC	GRADE	MANPOWER REQUIREMENT								
Comm-Computer Sys Supt	3C090	SMS							1	1	1
Comm-Comp Sys Ops Crftmn	3C071	MSG	1	1	1	1	1	1	1	1	1
Comm-Comp Sys Ops Crftmn	3C071	TSG					1	1	1	1	1
Comm-Comp Sys Ops Jrnymn	3C051	SSG	1	1	1	2	2	2	2	3	3
Comm-Comp Sys Ops Jrnymn	3C051	SRA	1	1	2	2	2	3	3	3	3
Comm-Comp Sys Ops Apr	3C031	AIC		1	1	1	1	1	1	1	2
TOTAL			3	4	5	6	7	8	9	10	11

AIR FORCE SPECIALTY TITLE	AFSC	GRADE	MANPOWER REQUIREMENT								
Comm-Computer Sys Supt	3C090	SMS	1	1							
Comm-Comp Sys Ops Crftmn	3C071	MSG	1	1							
Comm-Comp Sys Ops Crftmn	3C071	TSG	1	1							
Comm-Comp Sys Ops Jrnymn	3C051	SSG	3	3							
Comm-Comp Sys Ops Jrnymn	3C051	SRA	4	4							
Comm-Comp Sys Ops Apr	3C031	AIC	2	3							
TOTAL			12	13							

VARIANCES

Core Composition Variances. The following missions have been identified as variances. The impact for each of these variances can be determined by using the specific equations listed at the bottom of the attachment.

1. Title. Positive Mission Variance for Multiple User Computer System (includes LANs, MINIs, and Main Frames).

1.1. Definition. If there is a Multiple User Computer System located on the base use equation 1 to determine manpower requirement.

2. Title. Positive Mission Variance for NUCLEAR SURETY.

2.1. Definition. If the COMSEC account handles NUCLEAR SURETY material use equations 2 and 3 to determine manpower requirement.

3. Title. Positive Mission Variance for Airborne Command.

3.1. Definition. If the COMSEC account supports an Airborne Command Post use equations 2 and 3 to determine manpower requirement.

4. Title. Positive Mission Variance For CACHE Accounts.

4.1. Definition. If the COMSEC account supports a CACHE account use equations 2 and 3 to determine manpower requirement.

5. Title. Positive Mission Variance for Support of Republic of Korea (KR).

5.1. Definition. If the COMSEC account supports a KR requirement use equations 2 and 3 to determine manpower requirement.

6. Title. Positive Mission Variance for Any Special COMSEC requirements.

6.1. Definition. Workload associated with special COMSEC support to any agency not included in total base population (such as a contractor or special unit at a classified location with no base support except COMSEC) must be priced out utilizing equations 2 and 3 to determine manpower requirement.

7. Equations:

7.1. Variance Equation 1 = 2.22(X1)

X1 = Number of Multiple User Computer Systems (includes LANs, Minis, Main Frames)

7.2. Variance Equation 2 = 2.392(X2)

X2 = Number of COMSEC users.

7.3. Variance Equation 3 = .07268(X3)

X3 = Number of COMSEC Line Items

Application Instructions. Substitute the applicable workload factor (X1, X2, X3) to the appropriate equation. Add the resulting man-hours to the "Core" man-hours as described in paragraph 7 of the element manpower standard.

C4 SYSTEM SECURITY

PROCESS ANALYSIS SUMMARY

PROCESS TITLE	CORE MAN-HOURS	FRACTIONAL MANPOWER
COMPUTER SECURITY	128.99	0.81
TEMPEST	143.59	0.89
UNIT SECURITY	41.33	0.26
EDUCATION AND AWARENESS PROGRAM (ETAP)	11.27	0.07
COMSEC ACCT MGT	21.74	0.14
COMSEC OPERATIONS (CRYPTO)	127.8	0.8
SECURE TELEPHONE UNIT (STU-III)	85.38	0.53
ELEMENT TOTAL FRACTIONAL MANPOWER		3.50